Connecting Health Services with the Future: Guidance on Security and Privacy Issues for Clinicians

From 1 July 2011, Medicare and DVA Rebates and Financial Incentives will be available for telehealth under the Connecting Health Services with the Future initiative. This page contains information on security and privacy issues for telehealth.

The following information relating to security and privacy, interoperability and technical requirements is provided to assist healthcare providers in choosing telehealth (video conference) equipment.

Security and privacy

The following information has been taken from work commissioned by the Department to provide advice on security, privacy, interoperability and technical requirements for a broad range of telehealth services and will be dependent on individual clinical settings and requirements.

- To ensure public trust in a teleconsultation, privacy protection and security mechanisms must be integral to any implementation.
- Telehealth services should be compliant with all relevant state and federal laws.
- Telehealth service providers should periodically review and update their privacy policies to ensure that they adequately address the management of information gathered during telehealth consultations.
- Telehealth service providers should periodically review and update their privacy notices to ensure that they adequately address the management of information gathered during telehealth consultations.
- Telehealth service providers should periodically review and update their practices and procedures for managing personal information, including data security measures.
- Protocols used to secure telehealth consultations should be non-proprietary, standards-based to foster interoperability, inspectability and trust.
- Telehealth services, whether discrete practitioners or service providers should use a valid Public Key Infrastructure (PKI) certificate.
- The PKI certificate should be signed by a Certification Authority who maintains a Certificate Revocation List (CRL).
- The PKI certificate should use a minimum key strength e.g. 2048-bit encryption. As computing power increases then the level of encryption may need to be increased.
- PKI certificates should be stored in a physically or technically secured environment.
- All teleconsultation data (including ancillary data) must be secured for transmission across a data network either by use of encryption or VPN technology.
- All web services used in teleconsultations — including web-based video conferencing, patient records, messaging systems must be secured by a minimum Transport Layer Security Version 1.2.

- All emails containing patient data must be secured. This should be at a minimum by Secure Multipart Internet Mail Extensions (S/MIME) Version 3.0 or later and/or the latest technical specifications published by Standards Australia for E-Health Secure Message Delivery.
- Hardware based videoconferencing units must support International Telecommunications Union (ITU) H.235 standard allowing encrypted communication between end points in both point-to-point and multi-point videoconferencing sessions.
- The National Authentication Service or a similar service could be considered for telehealth service providers and telehealth applications when operational.
- All telehealth applications must enforce strong passwords.
- All telehealth applications support two-stage authentication.
- All telehealth applications record an audit trail of user's access to patient information.
- Policy guidelines for the retention and storage of telehealth records could be developed to assist those telehealth service providers which are not subject to specific legislative requirements for the retention and maintenance of health records.
- If storage is required, telehealth data (ancillary data and clinically determined recorded videoconference session) should be stored in a physically secure environment. The management (sanitisation, destruction and disposal) of media on which telehealth data is stored should be performed according to legislative obligations and sound technological practice. Secure storage is the responsibility of the telehealth service (including discrete practices, practitioners and service providers).
- If telehealth data is stored on a portable device it should be encrypted using a commercial data encryption application.

The decision to use, or not to use, telehealth together with the choice of particular hardware or software methods for consultation should rest with the clinician. In making their choices, clinicians should consider any legal (privacy and security), safety and clinical effectiveness implications.